

Common Mistakes for Enabling Security

Setting up Security with WebSphere Portal

- **I can not set up security with WebSphere Portal.**

Security could be enabled in a number of different ways and different level, parts, or components in WebSphere Application Server. You can go to the [WebSphere Portal Information Center](#) for more information on security concepts and procedures or way to setup security for WebSphere Portal.

Adding Security Programmatically

- **I can not create a form based login.**

Please refer to the [IBM WebSphere V5.0 Security Handbook](#) for the following steps on page 59, chapter 4.5.1 which will shows you how to configure form-based login using the Application Assembly Tool or WebSphere Studio.

For more information and details please refer to the [additional](#) resources related to this problem.

- **How can I programmatically secure EJBs**

J2EE security can be applied declaratively or programmatically. Programmatic security can be used by security aware applications when declarative security alone is not sufficient to express the security model of the application. The EJB 2.0 specification defines two methods that allow programmatic access to the caller's security context, `javax.ejb.EJBContext`.

- The `getCallerPrincipal` method allows the developer to get the name of the current caller.
- The `isCallerInRole` method allows the developer to make additional checks on the authorization rights of a user which are not possible or more difficult, to perform through the deployment descriptor of the EJB.

For more information and details please refer to the [additional](#) resources related to this problem.

- **Developing with JAAS to login programmatically**

To learn how to develop with JAAS to login programmatically click [here](#).

Additional Resources: [IBM Security Red Book](#) Chapter 8

Running Security as non-root user

- **I am trying to run as non-root with Local OS registry**

When running as non-root, if global security is enabled, the user registry must not be Local OS. Using the Local OS user registry requires the Application Server to run as root.

Please refer to the [document](#) for details.

- **Setting up Custom Registry using non root**

When running as non-root, you must use an LDAP or custom registry for the authentication mechanism for WebSphere security. Running as non-root under those situations is the same as running as root. Please refer to the [document](#) on how to setup a custom registry:

Global Security

- **Losing access to the Admin Console**

You can disable global security to gain access to Admin Console by using the following steps:

Go to your <installation_root>\AppServer\bin directory and execute the following command:

```
wsadmin -conntype NONE
```

At the `wsadmin>` prompt, enter `securityoff` and then type `exit` to return to a command prompt.

Restart the server.

- **Turning on and off Server level security with Network Deployment**

In WebSphere 5.0, when you enable global security without Network Deployment, you cannot set server level security separately. At the base level, it is similar to AEs at 4.0.x. When Network Deployment is installed and the node is federated, you will get the option of server level security in the administrative console under:

Servers / Application Servers / <servername> / Additional Properties/ Server Security / Server Level Security

This option does not exist unless the node is federated.

When you enable Global Security, Server level security is automatically enabled for all application servers. You can go into the previous area to turn off Server and Java 2 security.

Please refer to the [support document](#) for details.

- **After enabling single sign-on, I cannot log on to the administrative console**

This problem occurs when single signon (SSO) is enabled, and you attempt to access the administrative console using the short name of the server, for example <http://myserver:9090/admin>. The server accepts your user ID and password, but returns you to the log on page instead of the administrative console.

To correct this problem, use the fully qualified host name of the server, for example <http://myserver.mynetwork.mycompany.com:9090/admin>

- **I can not start the Application Server**

If you can not start the App Server using the local OS authentication username and password, it is possible that the password has been changed. Change the password back to the original and the server will start.

- **Errors messages when authenticating against Active Directory with global security enabled in Network Deployment environment**

Node may have been added without specifying -username and -password arguments. When global security is enabled, specifying the userid and password is required. Remove node and add node again with the -username and -password arguments. Please refer to the [AddNode](#) command details in the Network Deployment environment.

Some other common errors can be found in the Information Center's [Security troubleshooting section](#).

Trademarks and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	iSeries	OS/400	Informix	WebSphere
IBM(logo)	pSeries	AIX	Cloudscape	MQSeries
e(logo)business	xSeries	CICS	DB2 Universal Database	DB2
Tivoli	zSeries	OS/390	IMS	Lotus

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Microsoft, Windows, Windows NT, and

the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both. Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are

trademarks of Intel Corporation in the United States, other countries, or both. UNIX is a registered trademark of The Open Group in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.